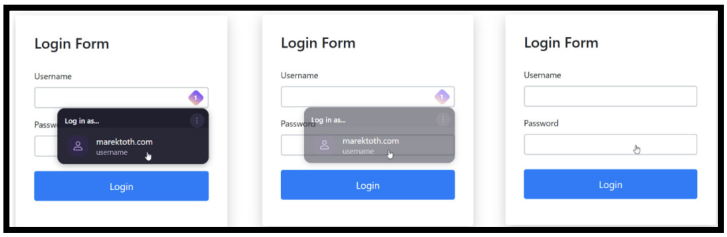
Critical Password Manager Updates

August 21, 2025

Executive Summary

At DEF CON 33, security researcher Marek Tóth unveiled a new class of vulnerabilities called **DOM-based extension clickjacking**, affecting browser plugins of major password managers. These flaws allow attackers to invisibly manipulate UI elements injected by extensions—such as autofill prompts—making them susceptible to credential theft with a single click. The attack works by embedding invisible login forms behind pop-ups, tricking users into triggering autofill actions that exfiltrate sensitive data like passwords, TOTP codes, and even passkeys.

As shown in the image below, threat actors can manipulate a website to change the transparency of an object. A video of the attack can be found here. Socket.dev independently reviewed Tóth's findings and confirmed the severity of the vulnerabilities. The firm noted that several vendors, including Bitwarden, Enpass, and iCloud Passwords, are working on fixes, while others like 1Password and LastPass have downplayed the issue as merely "informative."



However, 1Password released an update on August 20th and Bitwarden responded to information requests stating they will have an update released this week that addresses the vulnerability.

References

Cyber Insider: Zero-Day Clickjacking Flaws Found in Password Managers Used by Millions

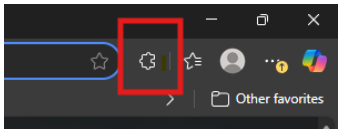
Socket: Researcher Exposes Zero-Day Clickjacking Vulnerabilities in Major Password Managers

The Hacker News: DOM-Based Extension Clickjacking Exposes Popular Password Managers to Credential and Data Theft

MarekToth: DOM Extension Clickjacking Demo 2

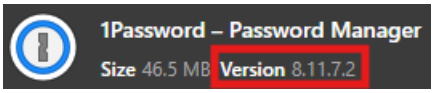
Recommendations

If you use a password manager, ensure you're using the most up-to-date version. To check this, click on the extension button as shown here:



Click the three dots to the right of your password manager and select Manage Extension.

Identify the Version you are running, as shown below:



If your version is earlier than those listed below, then run an update via the browser extension website.
1Password: 8.11.7.2 (20 August 2025)
Enpass: 6.11.6 (20 August 2025)

The following password managers are in the process of developing patches for the vulnerability:
iCloud Passwords: 3.1.25 (8 July 2025, patch is in progress)
Bitwarden: 2025.7.0 (24 July 2025, new update should be released within the next couple of days)

LastPass has no immediate plan to patch their extension, however, users should regularly check to see if an update is published.

Always keep critical extensions and applications up-to-date. This ensures they have the most recent patches and security updates, which contributes to your personal security and the overall security of the organization.

Contact Information

For questions or concerns regarding this notification, please contact us at phuwiler@abrguard.com

Warning: Do not click or navigate to any RED links or URLs within this document as they are known threat domains or IP addresses and provided for information purposes only.